Allied Telesis

AlliedWare Plus™ 5.3.4
Operating System

AlliedWare Plus™ OPERATING SYSTEM

AlliedWare Plus™ Layer 3 Fully Featured Operating System

The advanced **AlliedWare Plus™ Operating System** delivers a rich feature set and an industry-standard CLI. AlliedWare Plus is Allied Telesis' next generation operating system, providing advanced IPv4 and IPv6 features and even greater robustness and ease of management.

In keeping with the increasing complexity of Allied Telesis' ever-improving and feature-rich software, AlliedWare Plus employs a new modular approach to software creation and distribution. It represents a quantum shift in the software development methodology for Allied Telesis switches, providing you with even more features and greater robustness from the operating system.

The AlliedWare Plus operating system combines superior networking functionality and strong management capabilities with the exceptional performance that today's networks demand. A standards-based implementation, it also assures full interoperability with other major network equipment, along with improved usability and therefore a superior customer experience.

Modularity + Monitoring = Robust Flexibility

AlliedWare Plus has a modular architecture, providing superior reliability. It uses separate software processes, called modules, to handle different functions - for example management, routing protocols, and control functions. Each of these modules can only access its own allocated memory, which prevents processes from corrupting each other and causing system crashes. Although independent of each other, modules communicate via well-defined interfaces.

What's new?

- Dynamic Host Configuration Protocol (DHCP) Snooping
- sFlow
- VCStack Fast Failover
- Strong Passwords

For more information, go to page 2

Key Features

Easy to manage - The industry standard CLI reduces training requirements. With Virtual Chassis Stacking (VCStack™), units in a stack appear as one virtual chassis with a single IP address to simplify management.

Secure - Advanced security features protect your network - from the edge to the core. Network Access Control (NAC) gives unprecedented control over user access to your network.

Resilient - VCStack provides fast failover for uninterrupted network service. Sophisticated high availability features ensure traffic flow continues even during outages.

Future proof - Hardware-based IPv6 forwarding, along with 'IPv6 Ready' phase 2 certification, protects your investment. Licensing unlocks new features, and hot-swappable expansion modules (XEMs) enable network configuration flexibility.

Convergence - Comprehensive, low latency QoS features operating at wire-speed provide flow based traffic management.

AlliedWare Plus at a Glance:

AlliedWare Plus Advanced Features

- Industry Standard Command Line Interface (CLI)
- Virtual Chassis Stacking (VCStack)
- High Speed Stacking
- Network Access Control
- Highly Modular Software
- Superior Quality of Service (QoS)
- Policy-based Routing (PBR)
- 802.1x Dynamic VLAN Assignment
- Control Plane Prioritization (CPP)
- IPv6 Wirespeed Routing
- DHCP Snooping

Other Feature Highlights

- Loop Protection and Loop Detection
- Spanning Tree Protocol (STP) Root Guard
- Bridge Protocol Data Unit (BPDU) Protection
- Dynamic Link Failover
- Access Control Lists (ACLs)
- STP, RSTP, MSTP
- Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED)
- Ethernet Protection Switching Ring (EPSR)
- Virtual Router Redundancy Protocol (VRRP)
- Link Aggregation Control Protocol (LACP)
- Trigger Facility
- Logging Facility
- Scripting
- Web (HTTP) client
- Simple Mail Transfer Protocol (SMTP)
- Trivial File Transfer Protocol (TFTP) Client
- DHCP Server and Client
- Simple Network Management Protocol (SNMP)
- Internet Group Management Protocol (IGMP)
- IGMP Query Solicitation
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- RADIUS server
- NTP Master
- PIM-SM and PIM-DM
- Secure Copy (SCP)
- Advanced Storm Control
- GUI
- VLAN Double Tagging (Q-in-Q)
- Power over Ethernet (PoE)
- Policy-Based Routing (PBR)
- sFlow

What's new in Software Release 5.3.4

Dynamic Host Configuration Protocol (DHCP) Snooping

DHCP servers allocate IP addresses to clients, and the switch keeps a record of addresses issued on each port. IP Source Guard checks against this DHCP snooping database to ensure only clients with specific IP and/or MAC address can access the network. DHCP snooping can be combined with other features, like Dynamic ARP Inspection, to increase security in layer 2 switched environments, and also provides a traceable history, which meets the growing legal requirements placed on Service Providers.

sFlow

sFlow is an industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defence against security threats. Sampled packets sent to a collector ensure it always has a real-time view of network traffic.

VCStack Fast Failover

Virtual Chassis Stacking (VCStack) delivers resiliency and scalability to networks, simplifying management while increasing performance. Fast Failover further enhances this advanced solution by providing absolutely minimal network downtime in the event of a problem.

Strong Passwords

Enforcing strong passwords for users of key networking equipment allows network administrators to increase security, and ensure a robust and reliable infrastructure.

AlliedWare Plus Products

The following switches currently run the advanced AlliedWare Plus operating system:

- SwitchBlade® x908
- x900-24XT
- x900-24XT-N
- x900-24XS
- x900-12XT/S
- x600-24Ts
- x600-24Ts-POE
- x600-24Ts/XP
- x600-48Ts
- x600-48Ts/XP

Management

Industry Standard Command Line Interface (CLI)

The AlliedWare Plus operating system incorporates an industry standard CLI, facilitating intuitive manageability. Each command is associated with a specific function, or a common function performing a specific task. You can automate some of your configuration tasks, as many of these commands may also be used in scripts. Triggers can also be utilized, providing a powerful mechanism for automatic and timed management by automating the execution of commands in response to specific events.

With three distinct modes, the CLI is very secure. In User exec mode you can view settings and troubleshoot problems but you cannot make changes to the system. In Privileged exec mode you can change system settings and restart the device. You can only make configuration changes in Global configuration mode, which reduces the risk of making accidental configuration changes.

Virtual Chassis Stacking (VCStack™)

VCStack makes networking simple. It allows you to connect multiple switches together via high speed stacking links. This aggregates the switches, which then appear as a single switch, or 'virtual chassis'. The virtual chassis can be configured and managed via a single serial console or IP address, which provides greater ease of management in comparison to an arrangement of individually managed switches, and often eliminates the need to configure protocols like VRRP and Spanning Tree.

VCStack provides a highly available system where network resources can be spread out across the stacked switches, thus reducing the impact should one of the stacked switches fail. Ports on different switches across the stack can be aggregated to provide excellent link redundancy.

Graphic User Interface (GUI)

The GUI delivers maximum benefits with minimal complexity. Research shows that the GUI is most used for monitoring network status, rather than for performing configuration changes. As such, the AlliedWare Plus GUI provides extensive monitoring capabilities, and essential configuration capabilities.

Broadcast Forwarding

In a Wake on LAN environment, an L3 switch needs to forward the Wake on LAN broadcast packets across different subnets. Normal operation would limit the broadcast to all devices on the same subnet, but with Broadcast Forwarding, you can configure the L3 switch to allow broadcast packets to reach other subnets too.

IP Helper

When an L3 switch is configured as an IP Helper, the switch can relay broadcasts from clients in different subnets to their destination, instead of blocking them. With IP Helper, Windows client machines can be on a different subnet to the Windows server, and NetBIOS broadcasts that are fundamental to the Windows network can still successfully pass between the switches.

Security

802.1x, RADIUS Authentication and Dynamic VLAN Assignment

The IEEE 802.1x standard manages port-based network access. It provides authentication to devices attached to a LAN port by initiating a connection or preventing access if authentication fails. Valuable for authenticating and controlling user traffic to a protected network, 802.1x is also effective for dynamically varying encryption keys. 802.1x attaches the Extensible Authentication Protocol (EAP) to both wired and wireless LAN media, and supports multiple authentication methods, such as token cards, Kerberos, certificates, and public key authentication.

802.1x uses the RADIUS (Remote Authentication Dial In User Service) protocol to transfer authentication and configuration information between the switch and a shared RADIUS authentication Server, which manages a database of users and provides authentication and configuration information to the client.

Dynamic VLAN assignment allows an 802.1x supplicant to be placed into a specific VLAN based on information returned from the RADIUS server during authentication. This limits a supplicant's network access to a specific VLAN, and prevents supplicants from connecting to VLANs for which they are not authorized.

Network Access Control (NAC)

NAC provides unprecedented control over user access to the network, in order to mitigate threats to network infrastructure. NAC uses 802.1x port-based authentication with standards-compliant dynamic VLAN assignment, to assess a user's adherence to the network's security policies, and either grant authentication or offer remediation.

NAC also supports alternatives to 802.1x port-based authentication, such as web authentication to enable guest access, and MAC authentication for end points that do not have an 802.1x supplicant. Furthermore, if multiple users share a port then multi-authentication can be used and a Guest VLAN (also known as Default VLAN) can be configured to provide a catch-all for users without an 802.1x supplicant.

Secure Shell (SSH) version 2 (SSHv2)

SSH provides encrypted and strongly authenticated remote login sessions. SSHv2 provides sessions between a host running an SSH server and a machine with an SSH client.

Secure Copy Protocol (SCP)

SCP allows for secure file transfer to and from the switch, protecting your network from unwanted downloads and unauthorized file copying.

Access Control Lists (ACLs)

AlliedWare Plus delivers industry-standard Access Control functionality through access control lists (ACLs). ACLs filter network traffic to control whether packets are forwarded or blocked at the port interface. The switch examines each packet to determine whether to forward or drop the packet based on the criteria that is specified within the ACL, such as source and destination MAC or IP address, IP protocol, or TCP/UDP port. This provides a powerful network security mechanism to select the types of traffic to be analyzed, forwarded, or influenced in some way, for example to restrict routing updates or provide traffic flow control.

Bridge Protocol Data Unit (BPDU) Protection

BPDU Protection adds extra security to the Spanning Tree Protocol (STP). It protects the spanning tree configuration by preventing malicious DoS attacks caused by spoofed BPDUs.

BPDU Protection is designed to be enabled on ports that should not receive BPDUs. These are edge ports connected to end user devices that do not run spanning tree. If a spoofed BPDU packet is received on a protected port, the BPDU Protection feature disables the port and alerts the network manager.

Spanning Tree Protocol (STP) Root Guard

STP Root Guard designates which devices can assume the role of Root Bridge in an STP network. This stops an undesirable device from taking over this role, where it could either compromise network performance or cause a security weakness.

Resiliency

Control Plane Prioritization (CPP)

The Control Plane Prioritization (CPP) feature allows you to allocate priorities to packet types, to ensure minimum interruption to the flow of control information through the network.

CPP stops the control plane from being flooded by traffic in the event of a network storm or Denial of Service (DoS) attack. This ensures maximal performance and prevents network outages.

Continued on next page

In addition, with CPP you can also limit the amount of traffic that flows to the CPU to ensure that performance of other services, such as the CLI, are not affected during network storms or DoS attacks.

Link Aggregation

Link aggregation allows a number of individual switch ports to be combined, forming a single logical connection of higher bandwidth. This provides a higher performance link, and also provides redundancy for a more reliable and robust network.

VCStack and Link Aggregation

Link Aggregation can be used across members of a stack to protect against link and device failures. This provides a resilient network solution that is easier to implement and administer than traditional redundant core networks. A VCStack solution in combination with Link Aggregation also achieves load balancing, as the stacked devices share the network traffic.

Virtual Router Redundancy Protocol (VRRP)

VRRP provides automatic backup in mission-critical environments. This feature enables multiple routers or switches to share a virtual IP address that serves as the default LAN gateway. Should the master fail, the other devices assume the virtual IP address. LAN devices can continue to be configured with a single default gateway address, and because VRRP is a standards based protocol, full interoperability with other VRRP-supported products is assured.

Storm Protection

Advanced packet storm control features protect your network from broadcast storms:

- Bandwidth limiting minimises the effects of the storm by reducing the amount of flooding traffic.
- Policy-based storm protection is more powerful than bandwidth limiting. It lets you restrict storm damage to within the storming VLAN, and it gives you the flexibility to define the traffic rate that creates a broadcast storm. You can also configure the action the device should take when it detects a storm, such as disabling the port from the VLAN or shutting the port down.
- Packet storm protection allows you to set limits on the broadcast reception rate, multicast frames and destination lookup failures. In addition, you can set separate limits to specify when the device will discard each of the different packet types.

Ethernet Protected Switching Ring (EPSR)

EPSR allows several switches to form a protected ring with sub 50ms failover. This feature is perfect for high performance at the core of enterprise or provider access networks.

MSTP - Multiple Spanning Tree Protocol

MSTP addresses the limitations in the existing spanning tree protocols, Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). MSTP is similar to RSTP in that it provides loop resolution and rapid convergence. However it also has the significant extra advantage of making it possible to have different forwarding paths for different multiple spanning tree instances. This enables load balancing of network traffic across redundant links.

Loop Protection

AlliedWare Plus provides two forms of Loop Protection, Thrash Limiting and Loop Detection:

Thrash Limiting, also known as Rapid MAC Movement, detects and resolves network loops. It is highly user-configurable - from the rate of looping traffic to the type of action the switch should take when it detects a loop.

Loop Detection works in conjunction with Thrash Limiting. With Thrash Limiting, the switch only detects a loop when a storm has occurred, which can potentially cause disruption to the network. To avoid this, Loop Detection sends special packets that the switch listens for. You can specify an action to apply to a port that sends a special packet. You can choose to either disable the port, disable the link, or send an SNMP trap.

Dynamic Link Failover

Dynamic Link Failover (Host Attach) is a versatile feature that enables devices that do not support link aggregation to form multiple active links, by using triggers and scripts. You can customize Dynamic Link Failover to suit almost any situation, from a simple redundant backup link to multiple active links capable of basic load-sharing.

Future-proofing

IPv6 Wirespeed Forwarding

As the IPv4 address space diminishes, IPv6 is rapidly becoming a mandatory requirement for many government and enterprise customers. To meet this need now and into the future, AlliedWare Plus enables IPv6 forwarding in hardware on all supported platforms.

We provide a comprehensive suite of routing and management features, delivering future-proof networking while retaining your existing IPv4 network infrastructure.

Our IPv6 features include:

- Wirespeed IPv6 unicast forwarding and routing in hardware
- Static routing and RIPng
- "Dual stack" for simultaneous IPv4 and IPv6 traffic processing
- Tunnelling enabling IPv4 traffic forwarding over an IPv6 network
- MLD Snooping for efficient bandwidth use when serving MLD streams

AlliedWare Plus Licensing Unlocks New Features

With AlliedWare Plus, a single license password or 'key' is all that is necessary to "unlock" additional feature bundles that ship with the switches.. This single key enables the bundled features on all hardware of that particular product type.

Hot-swappable XEM modules

The AlliedWare Plus operating system supports hot-swappable XEM modules, dramatically reducing system downtime. You can remove and add XEM modules, or swap a XEM for another of the same sort - all without having to reboot or reconfigure your network.

Convergence

Policy-Based Quality of Service (QoS)

Comprehensive, low latency QoS features operating at wire-speed provide flow based traffic management with full classification, prioritization, traffic shaping and min/max bandwidth profiles.

Our QoS features are ideal for service providers wanting to ensure maximum availability of premium voice, video and data services, and at the same time manage customer service level agreements. For enterprise customers, the QoS features protect productivity by guaranteeing performance of business-critical applications (including VoIP services), and help to restore and maintain responsiveness of enterprise applications in the workplace.

MLD Snooping

MLD Snooping reduces the amount of multicast traffic on a network by sending the streams only to interested recipients, instead of flooding to all recipients. This results in far more efficient use of network bandwidth.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP - MED)

LLDP-MED extends LLDP's basic network endpoint discovery and management functions. LLDP-MED allows for media endpoint specific messages, providing detailed information on power requirements, network policy, location discovery (for Emergency Call Services) and inventory. LLDP-MED is an important feature for simplifying VOIP, security camera and WLAN deployments.

Voice VLAN

Voice VLAN automatically separates voice and data traffic into two different VLANS. This automatic separation places delay-sensitive traffic into a voice-dedicated VLAN, which simplifies QoS configurations.

AlliedWare Plus Operating System Features

Allied Telesis Product	x600	x900	AT-SBx908
Software Release	5.3.4	5.3.4	5.3.4
Resiliency			
STP - *Spanning Tree Protocol*	✓	✓	✓
RSTP - *Rapid Spanning Tree Protocol*	✓	✓	✓
MSTP (802.1s) - *Multiple Spanning Tree Protocol*	✓	✓	✓
EPSR - *Ethernet Protected Switched Rings*	✓	✓	✓
VRRP - *Virtual Router Redundancy Protocol*	✓	✓	✓
LACP - *Link Aggregation Control Protocol (802.3ad)*	✓	✓	✓
Storm Protection	✓	✓	✓
Virtual Chassis Stacking - VCStack	✓	✓	✓
Virtual Chassis Stacking Fast Failover	✓	✓	✓
CPP - *Control Plane Prioritization*	-	✓	✓
Security			
802.1x	✓	✓	✓
802.1x Dynamic VLAN Assignment	✓	✓	✓
Access Control Lists	✓	✓	✓
DoS Attack Prevention - *Denial of Service*	✓	-	-
Tri-Authentication (802.1x, MAC, web)	✓	✓	✓
802.1x Multi-supplicant	✓	✓	✓
Roaming Authentication	✓	✓	✓
SSHv2 - *Secure Shell version 2*	✓	✓	✓
RADIUS	✓	✓	✓
BPDU Protection - *Bridge Protocl Data Unit*	✓	✓	✓
Intrusion Detection (Port Security)	✓	✓	✓
Private VLANs	✓	✓	✓
DHCP Option 82 - *Dynamic Host Configuration Protocol*	✓	✓	✓
DHCP Snooping - *Dynamic Host Configuration Protocol*	✓	✓	✓
NAC - *Network Access Control*	✓	✓	✓
STP Root Guard - *Spanning Tree Protocol*	✓	✓	✓
Convergence			
Policy Based QoS -*Quality of Service*	✓	✓	✓
Strict Priority and/or WRR Queue Servicing - *Weighted Round Robin*	✓	✓	✓
LLDP- MED - *Link Layer Discovery Protocol Media Endpoint Discovery*	✓	✓	✓
Voice VLAN	✓	✓	✓
PoE Management - *Power over Ethernet*	✓	-	-
WRED Curves - *Weighted Random Early Discard*	-	✓	✓
Priority Tagging (IEEE 802.1p)	✓	✓	✓
Single-Rate Three-Color Marking	✓	✓	✓
Two-Rate Three-Color Marking	✓	✓	✓

✓ = Feature is available in the Standard AlliedWare release of this product
AL3 = Feature is available with the Advanced L3 feature license for this product
F = Feature will be available in a future release
IPv6 = Feature is available with the Advanced IPv6 feature license for this product

Note: This table does not provide a complete AlliedWare Plus® feature list. For more information about individual products, see www.alliedtelesis.com.

AlliedWare Plus Operating System Features table continued on the next page

AlliedWare Plus Operating System Features continued

Allied Telesis Product	x600	x900	AT-SBx908
Software Release	5.3.4	5.3.4	5.3.4
Convergence - continued			
IGMPv3 - *Internet Group Management Protocol*	✓	✓	✓
IGMP Proxy	✓	✓	✓
PIM-SM - *Protocol Independent Multicast Sparse Mode*	AL3	AL3	AL3
MLD Snooping	IPv6	IPv6	IPv6
PIM DM	AL3	AL3	AL3
IGMP Query Solicitation	✓	✓	✓
Network Manageability			
Industry Standard CLI - *Command Line Interface*	✓	✓	✓
RMON groups (1,2,3,9)	✓	✓	✓
HTTP Client	✓	✓	✓
TFTP Client - *Trivial File Transfer Protocol*	✓	✓	✓
SNMP - *Simple Network Management Protocol*	✓	✓	✓
Trigger Facility	✓	✓	✓
Scripting	✓	✓	✓
SCP - *Secure Copy*	✓	✓	✓
DHCP Client and Server- *Dynamic Host Configuration Protocol*	✓	✓	✓
Text Editor	✓	✓	✓
Telnet	✓	✓	✓
NTP - *Network Time Protocol*	✓	✓	✓
Ping Polling	✓	✓	✓
Syslog	✓	✓	✓
DHCP Relay	✓	✓	✓
DNS Client - *Domain Name System*	✓	✓	✓
GUI	✓	✓	✓
Dynamic Link Failover	✓	✓	✓
LLDP - *Link Layer Discovery Protocol*	✓	✓	✓
sFlow	✓	✓	✓
Routing			
Jumbo Frames	✓	✓	✓
VLAN Double Tagging (Q-in-Q)	AL3	AL3	AL3
OSPFv2 - *Open Shortest Path First*	AL3*	AL3*	AL3*
BGP-4 - *Border Gateway Protocol version 4*	AL3	AL3	AL3
RIPv1, RIPv2	✓	✓	✓
ECMP - *Equal Cost Multipath Protocol*	✓	✓	✓
Route Maps	✓	✓	✓
IP Helper	✓	✓	✓
Broadcast Forwarding	✓	✓	✓
IPv6 Static Routes	IPv6	IPv6	IPv6
RIPng	IPv6	IPv6	IPv6
Policy Based Routing	✓	✓	✓

* 64 Routes included in Base License

✓ = Feature is available in the Standard AlliedWare release of this product
AL3 = Feature is available with the Advanced L3 feature license for this product
F = Feature will be available in a future release
IPv6 = Feature is available with the Advanced IPv6 feature license for this product

Note: *This table does not provide a complete AlliedWare Plus® feature list. For more information about individual products, see www.alliedtelesis.com.*

Feature Licenses

Product	Advanced L3: • OSPF[1] • PIM-SM • PIM-DM • BGP4 • VLAN Double Tagging (Q in Q)	IPv6 Pack: • IPv6 Management • IPv6 Static Routes • IPv6 Unicast Forwarding • RIPng • MLD Snooping	RADIUS Full:[2] Store up to 5000 users and 1000 NAS in the local RADIUS database.
SwitchBlade® x908	AT-FL-SBX9-01	AT-FL-SBX9-02	AT-FL-RADIUS-FULL
x900-24XT	AT-FL-X900-01	AT-FL-X900-02	AT-FL-RADIUS-FULL
x900-24XT-N	AT-FL-X900-01	AT-FL-X900-02	AT-FL-RADIUS-FULL
x900-24XS	AT-FL-X900-01	AT-FL-X900-02	AT-FL-RADIUS-FULL
x900-12XT/S	AT-FL-X900-01	AT-FL-X900-02	AT-FL-RADIUS-FULL
x600-24Ts	AT-FL-X600-01	AT-FL-X600-02	AT-FL-RADIUS-FULL
x600-24Ts-POE	AT-FL-X600-01	AT-FL-X600-02	AT-FL-RADIUS-FULL
x600-24Ts/XP	AT-FL-X600-01	AT-FL-X600-02	AT-FL-RADIUS-FULL
x600-48Ts	AT-FL-X600-01	AT-FL-X600-02	AT-FL-RADIUS-FULL
x600-48Ts/XP	AT-FL-X600-01	AT-FL-X600-02	AT-FL-RADIUS-FULL

About Allied Telesis

Allied Telesis is part of the Allied Telesis Group. Founded in 1987, the company is a global provider of secure Ethernet/IP access solutions and an industry leader in the deployment of IP Triple Play networks over copper and fiber access infrastructure. Our POTS-to-10G iMAP integrated Multiservice Access Platform and iMG intelligent Multiservice Gateways, in conjunction with advanced switching, routing and WDM-based transport solutions, enable public and private network operators and service providers of all sizes to deploy scalable, carrier-grade networks for the cost-effective delivery of packet-based voice, video and data services.
Visit us online at www.alliedtelesis.com.

Service and Support

Allied Telesis provides value-added support services for its customers under its Net.Cover programs. For more information on Net.Cover support programs available in your area, contact your Allied Telesis sales representative or visit our website.

1 *64 OSPF Routes included in base software.*
2 *100 users and 24 NAS can be stored in local RADIUS database with the base software.*

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

www.alliedtelesis.com

© 2010 Allied Telesis Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners. 617-000477 Rev. N